

AMENDMENTS TO THE CLAIMS

This listing of the claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A data processing system for determining respective coefficients of at least part of at least a first polynomial of degree t in at least part of an inversion-free Berlekamp-Massey algorithm, wherein t is an integer, the system comprising:

a plurality of arithmetic units, each arithmetic unit comprising ~~at least one~~ a finite field multiplier and at least one finite field adder for selectively performing at least two finite field arithmetic calculations, such that the data processing system includes no more than (t+1) finite field multipliers;

means to use a previous finite field arithmetic calculation result of a first arithmetic unit of the plurality of arithmetic units in a current finite field arithmetic calculation of the first arithmetic unit; and

at least one finite field adder for combining respective finite field arithmetic calculation results of respective current finite field arithmetic calculations of at least two of the arithmetic units.

2. (Original) A data processing system as claimed in claim 1 in which a first arithmetic operation of the at least two arithmetic operations comprises a first finite field multiplication operation.

3. (Currently Amended) A data processing system as claimed in claim 2 in which the first finite field multiplication operation comprises calculating at least a first multiplication of $\delta\sigma^{(i-1)}(x)$ in a first clock cycle, where $\sigma^{(i-1)}(x)$ is an error locator polynomial at step (i-1) and δ is a previous step discrepancy, wherein i is an integer.

4. (Currently Amended) A data processing system as claimed in claim 2 in which the finite field arithmetic operation comprises calculating at least a second multiplication operation of $\Delta^{(i)}x\lambda^{(i-1)}(x)$ in a second clock cycle, where $\Delta^{(i)}$ is a step discrepancy at step i and $\lambda^{(i-1)}(x)$ is an auxiliary polynomial at step (i-1), wherein i is an integer.

5. (Original) A data processing system as claimed in claim 1 in which a second arithmetic operation of the at least two arithmetic operations comprises a finite field addition operation.

6. (Previously Presented) A data processing system as claimed in claim 5 in which the finite arithmetic addition operation comprises calculating at least part of $\delta\sigma^{(i-1)}(x)+\Delta^{(i)}x\lambda^{(i-1)}(x)$ as the current finite field arithmetic operation using $\delta\sigma^{(i-1)}(x)$ as at least part of the previous finite field arithmetic operation, where $\sigma^{(i-1)}(x)$ is an error locator polynomial at step (i-1), δ is a previous step discrepancy, $\Delta^{(i)}$ is a step discrepancy at step i and $\lambda^{(i-1)}(x)$ is an auxiliary polynomial at step (i-1).

7. (Previously Presented) A data processing system as claimed in claim 1 further comprising the plurality of arithmetic units operable substantially in parallel to calculate respective coefficients of at least part of at least a first polynomial.

8. (Previously Presented) A data processing system as claimed in claim 7 in which the first polynomial comprises at least $\delta\sigma^{(i-1)}(x)+\Delta^{(i)}x\lambda^{(i-1)}(x)$, where $\sigma^{(i-1)}(x)$ is an error locator polynomial at step (i-1), δ is a previous step discrepancy, $\Delta^{(i)}$ is a step discrepancy at step i and $\lambda^{(i-1)}(x)$ is an auxiliary polynomial at step (i-1).

9. (Original) A data processing system as claimed in claim 1 in which the at least two arithmetic calculations comprises a second finite field multiplication operation in a third clock cycle.

10. (Original) A data processing system as claimed in claim 9 in which the second finite field multiplication operation comprises calculating at least one coefficient of a second polynomial.

11. (Previously Presented) A data processing system as claimed in claim 9 in which the second arithmetic operation comprises calculating at least $S_{i-j+1}\sigma_j^{(i)}$, wherein S_{i-j+1} is coefficient i-j+1 of a syndrome polynomial and $\sigma_j^{(i)}$ is a coefficient j of an error locator polynomial at step i.

12. (Previously Presented) A data processing system as claimed in claim 11 in which the second arithmetic operation comprises calculating at least part of $\Delta^{(i+1)}=$

$S_{i+1}\sigma_0^{(i)}+S_i\sigma_1^{(i)}+\ldots+S_{i-t+1}\sigma_t^{(i)}$, where $\Delta^{(i+1)}$ is a step discrepancy at step (i+1) and S_i is coefficient i of a syndrome polynomial.

13. (Previously Presented) A data processing system as claimed in claim 1 comprising at least (t+1) such arithmetic units operable substantially in parallel, each unit producing respective coefficients of at least one of a first polynomial, $\sigma^{(i)}(x)=\delta\sigma^{(i-1)}(x)+\Delta^{(i)}x\lambda^{(i-1)}(x)$, and a step discrepancy, $\Delta^{(i+1)}=S_{i+1}\sigma_0^{(i)}+S_i\sigma_1^{(i)}+\ldots+S_{i-t+1}\sigma_t^{(i)}$, where $\sigma^{(i-1)})(x)$ is an error locator polynomial at step (i-1), δ is a previous step discrepancy, $\Delta^{(i-1)}(x)$ is a step discrepancy at step i, $\lambda^{(i-1)}(x)$ is an auxiliary polynomial at step (i-1) and S_i is coefficient of a syndrome polynomial.

14. (Original) A data processing system as claimed in claim 1 in which the first arithmetic unit is arranged to calculate at least a respective part of at least part of a further polynomial.

15. (Original) A data processing system as claimed in claim 14 in which the further polynomial is an error evaluator polynomial.

16. (Previously Presented) A data processing system as claimed in claim 14 in which calculating the further polynomial comprises calculating

$$\begin{aligned}\Omega(x) &= S(x)\sigma(x) \bmod x^{2t}\\ &= (S_0+S_1x+\ldots+S_{2t-1}x^{2t-1})\cdot(\sigma_0+\sigma_1x+\ldots+\sigma_tx^t) \bmod x^{2t}\\ &= \Omega_0+\Omega_1x+\ldots+\Omega_{t-1}x^{t-1}, \text{ where}\end{aligned}$$

$\Omega_i = S_i\sigma_0+S_{i-1}\sigma_1+\ldots+S_{i-t+1}\sigma_{t-1}$, where $i = 0,1,\ldots,t-1$, and where $\Omega(x)$ is an error evaluator polynomial, s(x) is a syndrome polynomial and $\sigma(x)$ is an error locator polynomial.

17. (Previously Presented) A data processing system as claimed in claim 14 in which the at least a respective part of at least part of the further polynomial comprises calculating:

$\Omega_i = \Omega_i^{(t-1)}$, where

$\Omega_i^{(j)} = S_i\sigma_0$, for j = 0; and

$\Omega_i^{(j)} = \Omega^{(j-1)}+S_{i-j}\sigma_j$, for $1\leq j \leq t\text{-}1\cancel{i}$,

where Ω_i is coefficient I of an error evaluator polynomial $\Omega(x)$, S_i is coefficient I of a syndrome polynomial S(x) and σ_i is coefficient I of an error locator polynomial σ (x).

Claims 18-20. (Canceled)

21. (Previously Presented) A data processing system as claimed in claim 14 wherein $\Omega(x)$ is calculated in t clock cycles.

22. (Previously Presented) A data processing system as claimed in claim 3, wherein the error locator polynomial $\sigma(x)$ is calculated in 6t clock cycles.

23. (Previously Presented) A data processing system as claimed in claim 8, wherein the error locator polynomial $\sigma(x)$ is calculated in 6t clock cycles.

24. (New) A data processing system as claimed in claim 1, further comprising (2t+1) finite filed adders.